

REMARKS

Applicant respectfully requests reconsideration and allowance of the subject application. Claim 8 has been amended. Claim 10 has been canceled without prejudice. Claims 1-9 and 11-36 are pending in this application.

35 U.S.C. § 103

Claims 1-6, 8-13, and 15-30 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,003,597 to Merkle (hereinafter "Merkle") in view of U.S. Patent No. 6,594,761 to Chow et al. (hereinafter "Chow"). Claim 10 has been canceled without prejudice. Applicant respectfully submits that claims 1-6, 8-9, 11-13, and 15-30 are not obvious over Merkle in view of Chow.

Merkle is directed to method and apparatus for data encryption (see, Title). As discussed with reference to Figures 1 and 2 of Merkle, as well as the Abstract, the method uses part of the data input to access a table of pseudo-random numbers. The pseudo-random numbers are exclusively ORed (XORed) with the remaining part of the data input. The output from the XOR operation is then used to access the table where the other portion of the data is in turn XORed with the pseudo random numbers. This iterative process continues until the data is fully randomized.

Chow is directed to tamper resistant software encoding (see, Title). As discussed in the Abstract of Chow, the method of the invention is to increase the tamper-resistance and obscurity of computer software code by transforming the data flow of the computer software so that the observable operation is dissociated

from the intent of the original software code. A number of techniques for performing the invention are given, including encoding software arguments using polynomials, prime number residues, converting variables to new sets of Boolean variables, and defining variables on a new n-dimensional vector space.

With respect to claim 1, claim 1 recites:

One or more computer readable media having stored thereon a plurality of instructions that, when executed by one or more processors, causes the one or more processors to perform acts including:

- selecting a portion of a digital good;
- selecting another portion of the digital good, wherein the other portion is to be encrypted; and
- using the portion as a substitution box (S-box) when encrypting the other portion.

Applicant respectfully submits that Merkle in view of Chow does not disclose or suggest selecting a portion of a digital good and using the portion as a substitution box as recited in claim 1.

In the May 5 Office Action at pages 2-3, Merkle is cited as teaching this selecting and using of claim 1. Applicant respectfully disagrees with this characterization. The cited portions of Merkle (Fig. 1 and col. 2, line 51 – col. 3, line 21) discuss that data is processed in 64-bit clear text blocks (see, col. 2, line 53). The initial 64-bit clear text block is split in half, creating an initial left half L_{-1} of 32 bits and an initial right half R_{-1} of 32 bits (see, col. 2, lines 53-56). These values are XORed with a 32-bit Auxiliary key 0 and 32 bit Auxiliary Key 1, and the output from this operation is an initial left half L_0 and an initial right half R_0 , each 32 bits in length (see, col. 2, lines 56-63). The rightmost eight bits of L_0 are used as an input to an S-box (see, emphasis added, col. 2, lines 64-66). The output from the S-box is a 32 bit entry which is then XORed with R_0 (see, col. 2, lines

66-67). L_0 is then rotated according to a predefined rotation schedule, and after its rotation the 32-bit word is labeled R_1 and used as the right half input in the next iteration of the encryption method (see, col. 2, line 67 – col. 3, line 3). The output from the XOR operation of R_0 and the S-box entry is labeled L_1 and used as the left half input in the next iteration of the encryption method (see, col. 3, lines 3-6).

Thus, the cited portions of Merkle discuss portions of a 64-bit clear text block being used to calculate an input to an S-box, not being used as the S-box itself. Nowhere in the cited portions of Merkle, or elsewhere in Merkle, is there any discussion or even mention of using the 64-bit clear text block itself as the S-box. As such, the cited portions of Merkle cannot disclose or suggest selecting a portion of a digital good and using the portion as a substitution box as recited in claim 1.

Merkle does go on to discuss computation of an S-box by pre-computing an S-box in a pseudo-random fashion from a user supplied key, satisfying a property that all four of the one-byte (8-bit) columns in the S-box must be permutations of one another (see, col. 4, lines 46-54). The pre-computation of a pseudo-random S-box satisfying the desired properties can be divided into two stages: first, a stream of pseudo-random bytes is generated; second, the stream of pseudo-random bytes is used to generate four pseudo-random permutations that map 8 bits to 8 bits (see, col. 5, lines 1-6). These four pseudo-random permutations are the generated S-box (see, col. 5, lines 6-7).

However, such discussions of computation of an S-box make no mention whatsoever of selecting a portion of a digital good and using the portion as a substitution box. As such, Applicant respectfully submits that Merkle cannot

disclose or suggest selecting a portion of a digital good and using the portion as a substitution box as recited in claim 1.

With respect to Chow, Chow is cited in the May 5 Office Action at p. 3 for “using DES technique to obfuscate digital good for tamper resistant protection”. Applicant respectfully submits that Chow is not cited as curing, and does not cure, these deficiencies of Merkle.

For at least these reasons, Applicant respectfully submits that claim 1 is allowable over Merkle in view of Chow.

With respect to claims 2-6, given that claims 2-6 depend from claim 1, Applicant respectfully submits that claims 2-6 are likewise allowable over Merkle in view of Chow for at least the reasons discussed above with respect to claim 1.

With respect to amended claim 8, Applicant respectfully submits that, similar to the discussion above regarding claim 1, Merkle in view of Chow does not disclose or suggest mapping, as at least part of the encryption process, values within the other segment to new values based on the segment, wherein the mapping comprises using the segment as a substitution box (S-box) during the encryption process as recited in amended claim 8. For at least these reasons, Applicant respectfully submits that amended claim 8 is allowable over Merkle in view of Chow.

With respect to claims 9, 11-13, and 15-16, given that claims 9, 11-13, and 15-16 depend from amended claim 8, Applicant respectfully submits that claims 9, 11-13, and 15-16 are likewise allowable over Merkle in view of Chow for at least the reasons discussed above with respect to amended claim 8.

With respect to claim 17, Applicant respectfully submits that, similar to the discussion above regarding claim 1, Merkle in view of Chow does not disclose or suggest using at least a portion of a digital good as a substitution box (S-box) as recited in claim 17. For at least these reasons, Applicant respectfully submits that claim 17 is allowable over Merkle in view of Chow.

With respect to claims 18-24, given that claims 18-24 depend from claim 17, Applicant respectfully submits that claims 18-24 are likewise allowable over Merkle in view of Chow for at least the reasons discussed above with respect to claim 17.

With respect to claim 25, Applicant respectfully submits that, similar to the discussion above regarding claim 1, Merkle in view of Chow does not disclose or suggest a production server being configured to identify a first segment in the original program and use the first segment as an S-box when encrypting a second segment of the original program as recited in claim 25. For at least these reasons, Applicant respectfully submits that claim 25 is allowable over Merkle in view of Chow.

With respect to claims 26-30, given that claims 26-30 depend from claim 25, Applicant respectfully submits that claims 26-30 are likewise allowable over Merkle in view of Chow for at least the reasons discussed above with respect to claim 25.

Claims 31-36 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Merkle in view of U.S. Patent No. 5,809,144 to Sirbu et al. (hereinafter "Sirbu"). Applicant respectfully submits that claims 31-36 are not obvious over Merkle in view of Sirbu.

Sirbu is directed to a method and apparatus for purchasing and delivering digital goods over a network (see, Title). As discussed in the Abstract of Sirbu, the method includes identifying a digital good to be purchased. A purchase price for the digital good is negotiated. After the negotiation step, an authenticated purchase request is sent to the merchant. The merchant encrypts the desired digital good and calculates a first cryptographic checksum for the encrypted good. The encrypted digital good and the first cryptographic checksum together with a timestamp are then transmitted to the customer. The customer calculates a second cryptographic checksum for the received encrypted digital good. The customer creates an electronic payment order containing information identifying the transaction, the second cryptographic checksum, credentials, and the timestamp. The electronic payment order is transmitted to the merchant. The merchant compares the first and second cryptographic checksums to ensure that they match, and if so, the merchant adds an electronic signature and a decryption key to the electronic payment order. The merchant submits the merchant signed electronic payment order and the key to an account server for review. The account server reviews the information in the electronic payment order and sends a message, including the key if the review is positive, to the merchant. The merchant forwards the message to the customer. If the message contained the key, the customer uses the key to decrypt the goods.

With respect to claim 31, claim 31 recites:

A client-server system, comprising:
a production server to use a portion of a first digital good as a substitution box (S-box) in encrypting at least a portion of a second digital good to produce a protected digital good; and

a client to store and execute the protected digital good, the client being configured to evaluate the protected digital good to determine whether the protected digital good has been tampered with.

Applicant respectfully submits that Merkle in view of Sirbu does not disclose or suggest a production server to use a portion of a first digital good as a substitution box (S-box) in encrypting at least a portion of a second digital good to produce a protected digital good as recited in claim 1.

In the May 5 Office Action at page 5, Merkle is cited as teaching “Selecting portion of clear text as a substitution box (S-box) in encrypting at least a portion of a second portion of clear text to produce encrypted text (see col. 2, line 52-col. 3, line 35)”. However, similar to the discussion above regarding claim 1, Applicant respectfully submits that Merkle does not disclose or suggest a production server to use a portion of a first digital good as a substitution box (S-box) in encrypting at least a portion of a second digital good to produce a protected digital good as recited in claim 1.

With respect to Sirbu, Sirbu is cited in the May 5 Office Action at p. 5 as teaching “a server production encrypts digital good; and a client to store and execute the protected digital good, the client being configured to evaluate the protected digital to determine whether the protected digital good has been tampered with”. Applicant respectfully submits that Sirbu is not cited as curing, and does not cure, these deficiencies of Merkle.

For at least these reasons, Applicant respectfully submits that claim 31 is allowable over Merkle in view of Sirbu.

With respect to claim 32, given that claim 32 depends from claim 31, Applicant respectfully submits that claim 32 is likewise allowable over Merkle in view of Sirbu for at least the reasons discussed above with respect to claim 31.

With respect to claim 33, Applicant respectfully submits that, similar to the discussion above regarding claim 31, Merkle in view of Sirbu does not disclose or suggest decrypting at least a portion of a digital good by using another portion of the digital good as a substitution box (S-box) as recited in claim 33. For at least these reasons, Applicant respectfully submits that claim 33 is allowable over Merkle in view of Sirbu.

With respect to claims 34-36, given that claims 34-36 depend from claim 33, Applicant respectfully submits that claims 34-36 are likewise allowable over Merkle in view of Sirbu for at least the reasons discussed above with respect to claim 33.

Claims 7 and 14 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Merkle in view of Chow and further in view of Sirbu. Applicant respectfully submits that claims 7 and 14 are not obvious over Merkle in view of Chow and further in view of Sirbu.

With respect to claim 7, claim 7 depends from claim 1 and Applicant respectfully submits that claim 7 is allowable over Merkle in view of Chow for at least the reasons discussed above with respect to claim 1. Applicant respectfully submits that Sirbu is not cited as curing, and does not cure, these deficiencies of Merkle in view of Chow. For at least these reasons, Applicant respectfully submits that claim 7 is allowable over Merkle in view of Chow and further in view of Sirbu.

With respect to claim 14, claim 14 depends from amended claim 8 and Applicant respectfully submits that claim 14 is allowable over Merkle in view of Chow for at least the reasons discussed above with respect to amended claim 8. Applicant respectfully submits that Sirbu is not cited as curing, and does not cure, these deficiencies of Merkle in view of Chow. For at least these reasons, Applicant respectfully submits that claim 14 is allowable over Merkle in view of Chow and further in view of Sirbu.

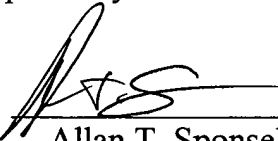
Applicant respectfully requests that the §103 rejections be withdrawn.

Conclusion

Claims 1-9 and 11-36 are in condition for allowance. Applicant respectfully requests reconsideration and issuance of the subject application. Should any matter in this case remain unresolved, the undersigned attorney respectfully requests a telephone conference with the Examiner to resolve any such outstanding matter.

Date: 8/5/04

Respectfully Submitted,

By: 
Allan T. Sponseller
Reg. No. 38,318
(509) 324-9256